# Constructions for Self-Dual Codes Induced from Group Rings

Joe Gildea
Department of Mathematics
Faculty of Science and Engineering
University of Chester, UK
j.gildea@chester.ac.uk

Abidin Kaya
Sampoerna Academy, L'Avenue Campus
12780, Jakarta, Indonesia
abidinkaya@mail.com

Rhian Taylor
Department of Mathematics
Faculty of Science and Engineering
University of Chester, UK
rhian.taylor@chester.ac.uk

Bahattin Yildiz
Department of Mathematics & Statistics
Northern Arizona University
Flagstaff, AZ 86001 USA
bahattin.yildiz@nau.edu

January 3, 2018

**Abstract**

In this work, we establish a strong connection between group rings and self-dual codes. We prove that a group ring element corresponds to a self-dual code if and only if it is a unitary unit. We also show that the double-circulant and four-circulant

constructions come from cyclic and dihedral groups, respectively. Using groups of order 8 and 16 we find many new construction methods, in addition to the well-known methods, for self-dual codes. We establish the relevance of these new constructions by finding many extremal binary self-dual codes using them, which we list in several tables. In particular, we construct 10 new extremal binary self-dual codes of length 68.

**Key Words**: Group rings; self-dual codes; codes over rings. **MSC 2010 Codes:** 94B05, 16S34

# 1 Introduction

There is a natural connection between algebraic codes and group rings. Using a map that was introduced by Hurley, to any group ring element, we can associate a matrix over the ring of coefficients, which then can be used to construct a linear code. Many of the properties of the codes can be obtained from the corresponding group ring elements. This connection has been explored in the literature to find new constructions for some well known codes such as the extended Golay code or the extended quadratic residue code. We refer the reader to [19], [18], [27], [28], [2] and the references therein for more on this connection.

Self-dual codes are a special class of codes that have connections to and applications in many fields such as Lattices, Designs, Cryptography, Invariant Theory, etc. The natural upper bound on the minimum distances of binary self-dual codes have led to the notion of extremal self-dual codes. There is a vast literature on construction and classification of extremal binary self-dual codes of certain lengths. Many different techniques have been utilized in finding extremal binary self-dual codes. A common theme in these methods of construction is the use of a computer search. In order to make this search feasible special construction methods have been used to reduce the search field. The double circulant, bordered double circulant and four circulant constructions are some of the methods by which many extremal binary self-dual codes have been obtained. While first applied over the binary field, these methods have also been applied over finite commutative rings of characteristic 2 with considerable success. For some of these constructions, we refer to [3], [20], [21], [22], [24], [25] and [30].

The motivation in this work is twofold: First, by using the strong connection between group ring elements and codes induced by Hurley's map, we find necessary and sufficient conditions on a group ring element whose corresponding code is self-dual. This brings a new motivation for studying the so-called "unitary units" in group rings. The second main result is that considering different groups in group rings lead to many new construction methods for self-dual codes. In particular we show that the double circulant, the four-circulant constructions are not some random constructions but that they come from certain

groups. By considering groups of orders 8 and 16, we come up with many new construction methods for self-dual codes. We illustrate the relevance of these constructions by finding many extremal binary self-dual codes, including ten new ones of length 68, by using them over appropriate group rings. We thus establish a new-found strong connection between group rings and Algebraic Coding Theory.

The rest of the paper is organized as follows: In Section 2, we recall some of the preliminaries on self-dual codes and some finite rings that we use in the subsequent chapters. In Section 3, we establish the connection between group ring elements and the corresponding self-dual codes. In Section 4 and 5, we list all the different constructions coming from groups of order 8 and 16, respectively. We find many extremal binary self-dual codes, using these constructions, which we list in several tables. In Section 6, we construct 10 new extremal binary self-dual codes of length 68. We finish the paper with some comments and possible directions for future study.

# 2 Preliminaries

We start by giving a background on binary self-dual codes and two rings that we will be using in the constructions.

## 2.1 Binary Self-dual Codes

A binary code $C$ of length $n$ is said to be self-dual if $C^{\perp} = C$. Self-dual codes are necessarily linear and self-orthogonal. Furthermore their dimension must be $n/2$, which means $n$ must be even. All codewords of a self-dual code have even weights. If all the weights of all codewords in the self-dual code $C$ are divisible by 4, then $C$ is called a Type II (or doubly even) code. Otherwise $C$ is called a Type I (singly even) code. Binary self-dual codes have bounds on their minimum distances:

**Theorem 2.1.** (*[29]*) *Let $d_I(n)$ and $d_{II}(n)$ be the minimum distance of a Type I and Type II binary code of length $n$, respectively. Then*

$$d_{II}(n) \leq 4\lfloor \frac{n}{24} \rfloor + 4$$

*and*

$$d_I(n) \leq \begin{cases} 4\lfloor \frac{n}{24} \rfloor + 4 & \text{if } n \not\equiv 22 \pmod{24} \\ 4\lfloor \frac{n}{24} \rfloor + 6 & \text{if } n \equiv 22 \pmod{24}. \end{cases}$$

Self-dual codes meeting these bounds are called *extremal*. Finding extremal binary self-dual codes of certain lengths is a relevant problem in Coding Theory, that attracts a lot of attention.

## 2.2 The rings $\mathbb{F}_2 + u\mathbb{F}_2$ and $\mathbb{F}_4 + u\mathbb{F}_4$

Different rings have recently been studied within the context of codes as they have extended the tools of classical coding theory. The construction methods introduced in this work can be applied to rings with successful results. We will illustrate this idea on two particular rings that have been used in this context before.

Both the rings $\mathbb{F}_2 + u\mathbb{F}_2$ and $\mathbb{F}_4 + u\mathbb{F}_4$ are finite commutative rings of characteristic 2 with one non-trivial ideal, that is the ideal $\langle u \rangle$. The ring $\mathbb{F}_2 + u\mathbb{F}_2$ is designated as $R_1$ as it is the first case of an infinite family of rings denoted by $R_k$, described in more detail in [10].

Let $\mathbb{F}_4 = \mathbb{F}_2(\omega)$ be the quadratic field extension of $\mathbb{F}_2$, where $\omega^2 + \omega + 1 = 0$. The ring $\mathbb{F}_4 + u\mathbb{F}_4$ is defined via $u^2 = 0$. Note that $\mathbb{F}_4 + u\mathbb{F}_4$ can be viewed as an extension of $\mathbb{F}_2 + u\mathbb{F}_2$ and so we can describe any element of $\mathbb{F}_4 + u\mathbb{F}_4$ in the form $\omega a + \bar{\omega} b$ uniquely, where $a, b \in \mathbb{F}_2 + u\mathbb{F}_2$.

A code $C$ of length $n$ over $\mathbb{F}_4 + u\mathbb{F}_4$ is an $(\mathbb{F}_4 + u\mathbb{F}_4)$-submodule of $(\mathbb{F}_4 + u\mathbb{F}_4)^n$. With $\langle . \rangle_E$ denoting the Euclidean inner product, the dual $C^\perp$ of a code $C$ over $\mathbb{F}_4 + u\mathbb{F}_4$ can be defined as

$$C^\perp = \{x \in (\mathbb{F}_4 + u\mathbb{F}_4)^n \mid \langle x, y \rangle_E = 0 \text{ for all } y \in C\}.$$

A code $C$ is said to be self-dual if it is equal to its dual. In [13] and [11] the following Gray maps were introduced;

$$\begin{array}{l|l} \psi_{\mathbb{F}_4} : (\mathbb{F}_4)^n \to (\mathbb{F}_2)^{2n} & \varphi_{\mathbb{F}_2+u\mathbb{F}_2} : (\mathbb{F}_2 + u\mathbb{F}_2)^n \to \mathbb{F}_2^{2n} \\ a\omega + b\overline{\omega} \mapsto (a, b), \quad a, b \in \mathbb{F}_2^n & a + bu \mapsto (b, a + b), \quad a, b \in \mathbb{F}_2^n. \end{array}$$

Those were generalized to the following maps in [26];

$$\begin{array}{l|l} \psi_{\mathbb{F}_4+u\mathbb{F}_4} : (\mathbb{F}_4 + u\mathbb{F}_4)^n \to (\mathbb{F}_2 + u\mathbb{F}_2)^{2n} & \varphi_{\mathbb{F}_4+u\mathbb{F}_4} : (\mathbb{F}_4 + u\mathbb{F}_4)^n \to \mathbb{F}_4^{2n} \\ a\omega + b\overline{\omega} \mapsto (a, b), \quad a, b \in (\mathbb{F}_2 + u\mathbb{F}_2)^n & a + bu \mapsto (b, a + b), \quad a, b \in \mathbb{F}_4^n \end{array}$$

These maps preserve orthogonality in the corresponding alphabets. The binary images $\varphi_{\mathbb{F}_2+u\mathbb{F}_2} \circ \psi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$ and $\psi_{\mathbb{F}_4} \circ \varphi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$ are equivalent. The Lee weight of an element is defined to be the Hamming weight of its binary image.

**Proposition 2.2.** *([26]) Let $C$ be a code over $\mathbb{F}_4 + u\mathbb{F}_4$. If $C$ is self-orthogonal, so are $\psi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$ and $\varphi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$. $C$ is a Type I (resp. Type II) code over $\mathbb{F}_4 + u\mathbb{F}_4$ if and only if $\varphi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$ is a Type I (resp. Type II) $\mathbb{F}_4$-code, if and only if $\psi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$ is a Type I (resp. Type II) $\mathbb{F}_2 + u\mathbb{F}_2$-code. Furthermore, the minimum Lee weight of $C$ is the same as the minimum Lee weight of $\psi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$ and $\varphi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$.*

**Corollary 2.3.** *Suppose that $C$ is a self-dual code over $\mathbb{F}_4 + u\mathbb{F}_4$ of length $n$ and minimum Lee distance $d$. Then $\varphi_{\mathbb{F}_2+u\mathbb{F}_2} \circ \psi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$ is a binary $[4n, 2n, d]$ self-dual code. Moreover, $C$ and $\varphi_{\mathbb{F}_2+u\mathbb{F}_2} \circ \psi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$ have the same weight enumerator. If $C$ is Type I (Type II), then so is $\varphi_{\mathbb{F}_2+u\mathbb{F}_2} \circ \psi_{\mathbb{F}_4+u\mathbb{F}_4}(C)$.*

# 3 Construction methods induced from Group rings

In this section, we shall give a construction of codes in $R^n$ from the group ring $RG$. This construction was first given for codes over fields by Hurley in [18]. Let $R$ be a finite commutative Frobenius ring and let $G = \{g_1, g_2, \ldots, g_n\}$ be a group of order $n$. Let $v = \alpha_1 g_1 + \alpha_2 g_2 + \ldots \alpha_n g_n \in RG$. Define the matrix $\sigma(v) \in M_n(R)$ to be

$$\sigma(v) = \begin{pmatrix} \alpha_{g_1^{-1}g_1} & \alpha_{g_1^{-1}g_2} & \alpha_{g_1^{-1}g_3} & \ldots & \alpha_{g_1^{-1}g_n} \\ \alpha_{g_2^{-1}g_1} & \alpha_{g_2^{-1}g_2} & \alpha_{g_2^{-1}g_3} & \ldots & \alpha_{g_2^{-1}g_n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha_{g_n^{-1}g_1} & \alpha_{g_n^{-1}g_2} & \alpha_{g_n^{-1}g_3} & \ldots & \alpha_{g_n^{-1}g_n} \end{pmatrix}. \tag{1}$$

The elements $g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1}$ are simply the elements of the group $G$ in some order. We take this as the ordering of the elements since it makes the constructions more natural.

For a given element $v \in RG$, we define the following code over the ring $R$:

$$C(v) = \langle \sigma(v) \rangle, \tag{2}$$

that is the code formed by taking the row space of $\sigma(v)$ over the ring $R$.

We will now describe the general approach that we will utilize in finding construction methods for self-dual codes.

## 3.1 The General Idea

Let $G$ be a group of order $n$. We first give a labeling to the elements of the group by $G = \{g_1, g_2, \ldots, g_n\}$. Then for a given element $v = \alpha_1 g_1 + \alpha_2 g_2 + \cdots + \alpha_n g_n \in RG$ of the group ring, we look at the image of $v$ under the $\sigma$ map described above. Based on the structure of the group, these $n \times n$ matrices can have special block-structures. After figuring out what the block structure of $\sigma(v)$ is, we form the $n \times 2n$ matrix $[I_n | \sigma(v)]$. The code generated by this matrix will have size $|R|^n$. Thus if it is self-orthogonal, then we will have obtained a self-dual code. We can summarize this in the following main theorem:

**Theorem 3.1.** *Let $G$ be a group of order $n$ and $v = \alpha_1 g_1 + \alpha_2 g_2 + \cdots + \alpha_n g_n \in RG$ be an element of the group ring $RG$. The matrix $[I_n | \sigma(v)]$ generates a self-dual code over $R$ if and only if $\sigma(v)\sigma(v)^T = -I_n$.*

Using the previous theorem, we can relate self-dual codes to elements in a group ring in a strong way. To do this we recall the canonical involution $* : RG \to RG$ on a group ring $RG$ is given by $v^* = \sum_g a_g g^{-1}$, for $v = \sum_g a_g g \in RG$. An important connection between $v^*$ and $v$ appears when we take their images under the $\sigma$ map:

$$\sigma(v^*) = \sigma(v)^T. \tag{3}$$

Now using Theorem 3.1, the fact that $\sigma$ is a ring homomorphism and that $\sigma(v) = -I_n$ if and only if $v = -1$, we get the following corollary:

**Corollary 3.2.** *Let $RG$ be a group ring, where $R$ is a commutative Frobenius ring. For $v \in RG$, the matrix $[I_n|\sigma(v)]$ generates a self-dual code over $R$ if and only if $vv^* = -1$. In particular $v$ has to be a unit.*

When we consider a ring of characteristic 2, we have $-I_n = I_n$, which leads to the following further important result:

**Corollary 3.3.** *Let $RG$ be a group ring where $R$ is a commutative Frobenius ring of characteristic 2. Then the matrix $[I_n|\sigma(v)]$ generates a self-dual code over $R$ if and only if $v$ satisfies $vv^* = 1$, namely $v$ is a unitary unit in $RG$.*

There is a considerable amount of literature on unitary units of group rings. In particular the sizes and the descriptions of the unitary groups have been given for certain groups. This allows us to know exactly which elements in $RG$ would generate self-dual codes and also it will allow us to know exactly how many self-dual codes we could expect from a certain construction. As an example we illustrate this for a special case.

**Example 1.** *With $K$ denoting a ring of characteristic 2 and $G = D_{2^{n+1}}$, the Dihedral group of order $2^{n+1}$, Bovdi and Rosa calculated in [5] the size of the unitary group of $KG$ as $|K|^{3\cdot 2^{n-1}}$. This means, we can construct $|K|^{3\cdot 2^{n-1}}$ self-dual codes of length $2^{n+1}$ using elements in $KD_{2^{n+1}}$. As a particular case of this, which will appear in subsequent sections, we can take $G = D_8$ and $K = \mathbb{F}_{2^s}$. In this case, we will get $2^{6s}$ self-dual codes from elements in the group algebra $\mathbb{F}_{2^s}D_8$. In [15], Gildea characterized all unitary units of the group algebra $\mathbb{F}_{2^s}D_8$. He showed that the group of unitary units in this case is isomorphic to $C_2^{5s} \rtimes C_2^s$.*

*Now let us assume that $s = 1$. Then by [5] there are $2^6 = 64$ binary self-dual codes of length 16, coming from the group algebra $\mathbb{F}_2D_8$. Using the characterization given in [15], and searching through these elements, we see that eight of these self-dual codes have parameters $[16, 8, 2]$, while fifty-six of them are extremal self-dual codes, i.e. have parameters $[16, 8, 4]$.*

*If $s = 2$, we have $2^{12} = 4096$ quaternary self-dual codes of length 16 coming from the group algebra $\mathbb{F}_4D_8$. Considering the images of these self-dual codes under the duality-preserving Gray map, we get 4096 binary self-dual codes of length 32, eight of which have minimum distance 2, 1592 of which minimum distance 4, 1728 of which have minimum distance 6 and the remaining 768 are extremal, namely they are of parameters [32,16,8].*

Before moving on to the construction methods arising from certain groups, we would like to consider two special cases.

### 3.2 Two Special Cases

We would like to demonstrate, with the following examples, that many of the well-known construction methods in the literature of self-dual codes are just special cases of the idea we have described above.

If we take $G = C_n = \langle c \rangle$, the cyclic group of order $n$, then for $v = a_0e + a_1c + \cdots + a_{n-1}c^{n-1}$, we have $\sigma(v)$ is a circulant matrix. Thus the construction that is induced by the cyclic group is the well-known double-circulant construction, that has been oft-used in constructing self-dual codes.

If we take $G = D_{2n}$, the dihedral group of order $n$ and we label it as

$$G = \{e, x, \ldots, x^{n-1}, y, xy, \ldots, x^{n-1}y\},$$

then the companion matrix of a typical element $v \in RD_{2n}$ will be of the form

$$G = \begin{bmatrix} A & B \\ B^T & A^T \end{bmatrix},$$

which leads, when the characteristic of $R$ is 2, to another well-known construction method in the literature of self-dual codes, known as the four-circulant construction, when we put $I_{2n}$ next to it.

In what follows, we will take groups of order 8 and 16 to describe the construction methods arising from these groups for self-dual codes.

## 4 Constructions coming from groups of order 8

In this section, we will use Theorem 3.1 and Hurley's map to describe the construction methods coming from groups of order 8 and then the constructions will be applied to find extremal binary self-dual codes.

### 4.1 Constructions

For the groups below, we give the structure of the companion matrix $\sigma(v)$ for a typical element $v \in \mathbb{F}_2G$. We then take the matrices of the form $[I_8|\sigma(v)]$ to construct binary self-dual codes of length 16. Note that $cir(a_1, a_2, \ldots, a_n)$ means the circulant matrix whose first row is $(a_1, a_2, \ldots, a_n)$, while $rcir(a_1, a_2, \ldots, a_n)$ means the reverse circulant matrix. Let $CIR(A_1, A_2, \ldots, A_n)$ represent a block circulant matrix whose first row of block matrices are $A_1$, $A_2$,..., $A_n$. Additionally, let $P_\tau$ be the $n \times n$ permutation matrix for the permutation $\tau \in \mathcal{G}$ where $n = |\mathcal{G}|$.

▪ Let $G = \langle x_1, x_2, x_3 \,|\, x_i^2 = 1, x_jx_k = x_kx_j \ (j \neq k) \rangle \cong C_2^3$. If

$$\alpha = a_1 + a_2x_1 + a_3x_2 + a_4x_1x_2 + a_5x_3 + a_6x_1x_3 + a_7x_2x_3 + a_8x_1x_2x_3 \in RC_2^3,$$

then

$$\sigma(\alpha) = P_e \otimes CIR(A, B) + P_{(1,2)} \otimes CIR(C, D)$$

where $\mathcal{G} = \{e, (1, 2)\}$, $A = cir(a_1, a_2)$, $B = cir(a_3, a_4)$, $C = cir(a_5, a_6)$, $D = cir(a_7, a_8)$ and $a_i \in R$.

- Let $G = \langle x_1, x_2 \,|\, x^4 = y^2 = 1, xy = yx \rangle \cong C_2 \times C_4$. If

$$\alpha = \sum_{i=0}^{3} a_{i+1}x^i + a_{i+5}x^i y \in R(C_2 \times C_4),$$

then

$$\sigma(\alpha) = CIR(A, B)$$

where $A = cir(a_1, a_2, a_3, a_4)$, $B = cir(a_5, a_6, a_7, a_8)$ and $a_i \in R$.

- Let $G = \langle x, y \,|\, x^4 = y^2 = 1, xy = yx \rangle \cong C_2 \times C_4$. If

$$\alpha = \sum_{i=0}^{3} a_{2i+1}x^i + a_{2i+2}x^i y \in R(C_2 \times C_4),$$

then

$$\sigma(\alpha) = CIR(A, B, C, D)$$

where $A = cir(a_1, a_2)$, $B = cir(a_3, a_4)$, $C = cir(a_5, a_6)$, $D = cir(a_7, a_8)$ and $a_i \in R$.

- Let $G = \langle x, y \,|\, x^4 = y^2 = 1, x^y = x^{-1} \rangle \cong D_8$. If

$$\alpha = \sum_{i=0}^{3} a_{i+1}x^i + a_{i+5}x^i y \in RD_8,$$

then

$$\sigma(\alpha) = \begin{pmatrix} A & B \\ B^T & A^T \end{pmatrix}$$

where $A = cir(a_1, a_2, a_3, a_4)$, $B = cir(a_5, a_6, a_7, a_8)$ and $a_i \in R$. Note that this corresponds to the four-circulant construction when $char(R) = 2$, as we mentioned above.

- Let $G = \langle x, y \,|\, x^4 = y^2 = 1, x^y = x^{-1} \rangle \cong D_8$. If

$$\alpha = \sum_{i=0}^{3} a_{i+1}x^i + a_{i+5}yx^i \in RD_8,$$

then

$$\sigma(\alpha) = CIR(A, B)$$

where $A = cir(a_1, a_2, a_3, a_4)$, $B = rcir(a_5, a_6, a_7, a_8)$ and $a_i \in R$. This second construction from $D_8$ will be denoted by $D_8'$ in subsequent examples.

▪ Let $G = \langle x, y \mid x^4 = 1,\ y^2 = x^2,\ x^y = x^{-1} \rangle \cong Q_8$. If

$$\alpha = \sum_{i=0}^{3} a_{i+1}x^i + a_{i+5}yx^i \in RQ_8,$$

then

$$\sigma(\alpha) = \begin{pmatrix} A & B \\ C & A \end{pmatrix}$$

where $A = cir(a_1, a_2, a_3, a_4)$, $B = rcir(a_5, a_6, a_7, a_8)$, $C = rcir(a_7, a_8, a_5, a_6)$ and $a_i \in R$.

▪ Let $G = \langle x, y \mid x^4 = 1,\ y^2 = x^2,\ x^y = x^{-1} \rangle \cong Q_8$. If

$$\alpha = \sum_{i=0}^{3} a_{i+1}x^i + a_{i+5}x^iy \in RQ_8,$$

then

$$\sigma(\alpha) = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

where $A = cir(a_1, a_2, a_3, a_4)$, $B = cir(a_5, a_6, a_7, a_8)$, $C = cir(a_7, a_6, a_5, a_8)$, $D = cir(a_1, a_4, a_3, a_2)$ and $a_i \in R$. This second construction from $Q_8$ will be denoted by $Q_8'$ in subsequent examples.

## 4.2 Examples of Extremal Binary Self-dual Codes obtained from the constructions

We will focus on the new construction methods, with double-circulant and four-circulant cases being already done in the literature. We apply the constructions over the alphabets $\mathbb{F}_4 + u\mathbb{F}_4$, $\mathbb{F}_4$, $R_1$ and $\mathbb{F}_2$.

In [7] the possible weight enumerators for a self-dual Type I $[64, 32, 12]_2$-code were obtained in two forms as:

$$\begin{aligned} W_{64,1} &= 1 + (1312 + 16\beta)\, y^{12} + (22016 - 64\beta)\, y^{14} + \cdots, 14 \leq \beta \leq 284, \\ W_{64,2} &= 1 + (1312 + 16\beta)\, y^{12} + (23040 - 64\beta)\, y^{14} + \cdots, 0 \leq \beta \leq 277. \end{aligned}$$

Recently, 10 new codes with new weight enumerators in$W_{64,2}$ have been constructed in [20] by considering the $R_3$-lifts of the extended binary Hamming code. In [22], 15 new codes of length 64 with new weight enumerators have been constructed, and most recently in [1], 5 new codes were found. Together with these the existence of codes is known for $\beta$ =14, 16, 18, 20, 22, 24, 25, 26, 28, 29, 30, 32, 34, 35, 36, 38, 39, 44, 46, 53, 59, 60, 64 and 74 in $W_{64,1}$

Table 1: Extremal binary self-dual codes from $Q_8$

| $(a_1, a_2, a_3, a_4)$ | $(a_5, a_6, a_7, a_8)$ | $\lvert Aut(C)\rvert$ | Type |
|---|---|---|---|
| $(0,0,0,0)$ | $(0,1,1,1)$ | $2^{13} \times 3^2 \times 7^2$ | Type II |
| $(0,0,0,1)$ | $(1,1,1,1)$ | $2^{13} \times 3^2$ | Type I |
| $(0,1,1,1)$ | $(1,1,1,1)$ | $2^{14} \times 3^2 \times 5 \times 7$ | Type II |

and for $\beta$ =0,. . . , 18, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 32, 33, 34, 35, 36, 37, 38, 40, 41, 42, 44, 45, 48, 50, 51, 52, 56, 58, 64, 72, 80, 88, 96, 104, 108, 112, 114, 118, 120 and 184 in $W_{64,2}$.

Throughout the text extremal Type I binary self-dual codes of length 64 have weight enumerators in $W_{64,2}$. Hence, $\beta$ values in the upcoming tables correspond to $W_{64,2}$. In this section, we construct self-dual codes with weight enumerators $\beta$ =0, 2, 4, 6, 8, 9, 10, 12, 13, 14, 16, 17, 18, 20, 21, 24, 26, 28, 29, 30, 32, 36, 40, 44, 48 and 52 in $W_{64,2}$. Recently, codes with weight enumerators $\beta = 13,\ 17,\ 21,\ 26,\ 29$ and 52 in $W_{64,2}$ have been constructed in [20, 22] for the first time in the literature. We give an alternative construction for these.

The constructions emerging from groups of order 8 results in self-dual codes of length 16.

We need a brief notation for the elements of $\mathbb{F}_4 + u\mathbb{F}_4$. We use the ordered basis $\{u\omega, \omega, u, 1\}$ to express the elements of $\mathbb{F}_4 + u\mathbb{F}_4$ as binary strings of length 4, which then are transformed into the well-known hexadecimal notation. For instance, $1 + u\omega$ corresponds to 1001, which is represented by the hexadecimal 9.

**Example 2.** *Applying the first method of construction coming from the group $Q_8$ to the binary field, we get the following extremal binary self-dual codes of length 16: The same codes are also obtained from the second construction as well.*

In Table 2, extremal binary self-dual codes of length 64 have been constructed by $D_8'$ for $\mathbb{F}_4 + u\mathbb{F}_4$.

The results for the group $Q_8$ have been listed in Table 3.

**Example 3.** *We apply the construction method coming from $C_2^3$ over the binary case, with length* 16*. The results are listed in Table 4.*

**Example 4.** *We can apply these constructions to higher lengths as well. For example, if we take blocks of length* 4 *in the construction coming from $C_2^3$, we can get self-dual codes of length* 32*. Taking $A = cir(0,0,0,1)$, $B = cir(0,0,0,1)$, $C = cir(0,0,0,1)$ and $D = cir(1,1,1,1)$ in $C_2^3$ construction, we get the extremal Type II binary self-dual code of length* 8 *with automorphism group of order $2^9 \times 3^2 \times 5$.*

Table 2: The construction $D_8'$ over $\mathbb{F}_4 + u\mathbb{F}_4$

| $r_A$ | $r_B$ | $\lvert Aut(C)\rvert$ | $\beta$ |
|---|---|---|---|
| $(036E)$ | $(83B0)$ | $2^4$ | 0 |
| $(0FB4)$ | $(137E)$ | $2^5$ | 0 |
| $(2F34)$ | $(9BD6)$ | $2^4$ | 4 |
| $(16F1)$ | $(4455)$ | $2^5$ | 4 |
| $(3FC7)$ | $(4620)$ | $2^4$ | 8 |
| $(45BF)$ | $(C022)$ | $2^5$ | 8 |
| $(8AB1)$ | $(B6E8)$ | $2^4$ | 12 |
| $(66FF)$ | $(3846)$ | $2^5$ | 12 |
| $(6FC1)$ | $(8C09)$ | $2^4$ | 16 |
| $(6FB1)$ | $(03B0)$ | $2^4$ | 20 |
| $(773D)$ | $(F30B)$ | $2^4$ | 24 |
| $(996B)$ | $(8408)$ | $2^5$ | 24 |
| $(2DBE)$ | $(1174)$ | $2^4$ | 28 |
| $(CCDD)$ | $(B066)$ | $2^5$ | 28 |
| $(25B6)$ | $(91F4)$ | $2^4$ | 32 |
| $(3E2D)$ | $(B855)$ | $2^5$ | 32 |
| $(0C17)$ | $(648B)$ | $2^4$ | 36 |
| $(44FF)$ | $(984E)$ | $2^5$ | 36 |
| $(8FA8)$ | $(B47C)$ | $2^5$ | 40 |
| $(CCDD)$ | $(3AEC)$ | $2^5$ | 44 |
| $(66F5)$ | $(304C)$ | $2^4 \times 3$ | 44 |
| $(E65F)$ | $(1AC4)$ | $2^5$ | 48 |
| $(C47D)$ | $(90E6)$ | $2^5$ | 52 |

Table 3: The construction $Q_8$ over $\mathbb{F}_4 + u\mathbb{F}_4$

| $r_A$ | $r_B$ | $r_C$ | $\lvert Aut(C)\rvert$ | $\beta$ |
|---|---|---|---|---|
| $(55EE)$ | $(C522)$ | $(7E99)$ | $2^4$ | 0 |
| $(5FE6)$ | $(4F28)$ | $(2146)$ | $2^4$ | 2 |
| $(FFEE)$ | $(C7AA)$ | $(7C11)$ | $2^4$ | 4 |
| $(4273)$ | $(5E28)$ | $(6F19)$ | $2^3$ | 6 |
| $(F566)$ | $(1855)$ | $(A9E4)$ | $2^3$ | 8 |
| $(DBCA)$ | $(6EB8)$ | $(B365)$ | $2^3$ | 10 |
| $(DD44)$ | $(E588)$ | $(5E33)$ | $2^4$ | 12 |
| $(D544)$ | $(CF88)$ | $(A3E4)$ | $2^3$ | 14 |
| $(5FC4)$ | $(6D0A)$ | $(A9AE)$ | $2^4$ | 16 |
| $(7162)$ | $(CE10)$ | $(19C7)$ | $2^3$ | 18 |
| $(73E0)$ | $(6418)$ | $(3945)$ | $2^3$ | 20 |
| $(F7EE)$ | $(185F)$ | $(89CE)$ | $2^3$ | 26 |
| $(7D6E)$ | $(45A8)$ | $(DE33)$ | $2^5$ | 28 |
| $(55EE)$ | $(4F22)$ | $(5E33)$ | $2^4$ | 30 |

Table 4: Extremal binary self-dual codes from $C_2^3$

| $(a_1, a_2)$ | $(a_3, a_4)$ | $(a_5, a_6)$ | $(a_7, a_8)$ | $\lvert Aut(C)\rvert$ | Type |
|---|---|---|---|---|---|
| $(0,0)$ | $(0,0)$ | $(0,1)$ | $(1,1)$ | $2^{13} \times 3^2 \times 7^2$ | Type II |
| $(0,0)$ | $(0,1)$ | $(1,1)$ | $(1,1)$ | $2^{13} \times 3^2$ | Type I |
| $(0,1)$ | $(1,1)$ | $(1,1)$ | $(1,1)$ | $2^{14} \times 3^2 \times 5 \times 7$ | Type II |

Table 5: The construction $Q_8'$ over $\mathbb{F}_4 + u\mathbb{F}_4$

| $r_A$ | $r_B$ | $r_C$ | $r_D$ | $\lvert Aut(C)\rvert$ | $\beta$ |
|---|---|---|---|---|---|
| $(0577)$ | $(B179)$ | $(79B1)$ | $(7F0D)$ | $2^4$ | 8 |
| $(275F)$ | $(33F9)$ | $(519B)$ | $(7F07)$ | $2^3$ | 9 |
| $(2DFF)$ | $(9179)$ | $(D991)$ | $(7F8D)$ | $2^3$ | 12 |
| $(A57D)$ | $(33D9)$ | $(F913)$ | $(F72F)$ | $2^3$ | 13 |
| $(ADDF)$ | $(9BF3)$ | $(FB93)$ | $(DDAF)$ | $2^4$ | 16 |
| $(8D75)$ | $(9BD1)$ | $(F993)$ | $(DFA7)$ | $2^3$ | 17 |
| $(8F57)$ | $(915B)$ | $(5B31)$ | $(F50D)$ | $2^3$ | 21 |
| $(8F5D)$ | $(937B)$ | $(5911)$ | $(7587)$ | $2^3$ | 28 |
| $(07FF)$ | $(9359)$ | $(F913)$ | $(FF87)$ | $2^3$ | 29 |

The construction $Q_8'$ have been used for $\mathbb{F}_4 + u\mathbb{F}_4$ in Table 5

**Remark 1.** *The first examples of extremal binary self-dual codes of length* 64 *with weight enumerators* $\beta = 13,\ 17,\ 21,\ 26,\ 29$ *and* 52 *in* $W_{64,2}$ *have been recently constructed in [20, 22]. Those were constructed by using exhaustive search for the possible* $R_2$ *and* $R_3$*-lifts of binary self-dual codes of the corresponding lengths. We construct such codes in an alternative (and more direct) way by applying the constructions* $D_8'$*,* $Q_8$ *and* $Q_8'$ *to the ring* $\mathbb{F}_4 + u\mathbb{F}_4$*. Those have been listed in tables 2, 3 and 5. The binary generator matrices for these codes are available online at [16].*

# 5 Constructions coming from groups of order 16

In this section, we will apply the same approach that we used in the previous section to describe construction methods coming from groups of order 16 and to apply these construction methods to find extremal self-dual binary codes. For the constructions in this section, we need the definition of a so-called $g$-circulant matrix from [8]:

**Definition 1.** *Let* $0 \leq g \leq n$*. A* $g$*-circulant matrix* $B$ *of order* $n$ *is a matrix of the form*

$$B = g - circ(a_1, a_2, \ldots, a_n) = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_{n-g+1} & a_{n-g+2} & \cdots & a_{n-g} \\ a_{n-2g+1} & a_{n-2g+2} & \cdots & a_{n-2g} \\ \vdots & \vdots & \ddots & \vdots \\ a_{g+1} & a_{g+2} & \cdots & a_g \end{pmatrix}$$

*where each subscript are calculated* $\mod n$*.*

Note that,each row of $B$ is the previous row moved $g$ places to the right.

▪ Let $G = \langle x, y \mid x^4 = y^4 = 1,\ xy = yx \rangle \cong C_4 \times C_4$. If $\alpha = \sum_{i=0}^{3}\sum_{j=0}^{3} a_{1+i+4j}x^i y^j \in R(C_4 \times C_4)$, then

$$\sigma(\alpha) = CIR(A, B, C, D)$$

where $A = cir(a_1, a_2, a_3, a_4)$, $B = cir(a_5, a_6, a_7, a_8)$, $C = cir(a_9, a_{10}, a_{11}, a_{12})$, $D = cir(a_{13}, a_{14}, a_{15}, a_{16})$ and $a_i \in R$.

▪ Let $G = \langle x, y \mid x^4 = y^4 = 1,\ xyxy = 1,\ yx^3 = xy^3 \rangle \cong G_{4,4}$. If $\alpha = \sum_{i=0}^{3}\sum_{j=0}^{3} a_{1+i+4j}x^i y^j \in RG_{4,4}$, then

$$\sigma(\alpha) = CIR(A, B, C, D)$$

where $A = cir(a_1, a_2, a_3, a_4)$, $B = 3 - cir(a_5, a_6, a_7, a_8)$, $C = cir(a_9, a_{10}, a_{11}, a_{12})$, $D = 3 - cir(a_{13}, a_{14}, a_{15}, a_{16})$ and $a_i \in R$.

▪ Let $G = \langle x, y \mid x^4 = y^4 = 1,\ yx = x^{-1}y \rangle \cong C_4 \rtimes C_4$. If $\alpha = \sum_{i=0}^{3}\sum_{j=0}^{3} a_{1+i+4j}x^i y^j \in R(C_4 \rtimes C_4)$, then

$$\sigma(\alpha) = CIR(A, B, C, D)$$

where $A = cir(a_1, a_2, a_3, a_4)$, $B = rcir(a_5, a_6, a_7, a_8)$, $C = cir(a_9, a_{10}, a_{11}, a_{12})$, $D = rcir(a_{13}, a_{14}, a_{15}, a_{16})$ and $a_i \in R$.

▪ Let $G = \langle x, y \mid x^8 = y^2 = 1,\ xy = yx \rangle \cong C_2 \times C_8$. If $\alpha = \sum_{i=0}^{7}\sum_{j=0}^{1} a_{1+i+8j}x^i y^j \in R(C_2 \times C_8)$, then

$$\sigma(\alpha) = CIR(A, B)$$

where $A = cir(a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8)$, $B = cir(a_9, a_{10}, a_{11}, a_{12}, a_{13}, a_{14}, a_{15}, a_{16})$ and $a_i \in R$.

▪ Let $G = \langle x, y \mid x^8 = y^2 = 1,\ xy = yx \rangle \cong C_2 \times C_8$. If $\alpha = \sum_{i=0}^{7}\sum_{j=0}^{1} a_{1+2i+j}x^i y^j \in R(C_2 \times C_8)$, then

$$\sigma(\alpha) = CIR(A, B, C, D, E, F, G, H)$$

where $A = cir(a_1, a_2)$, $B = cir(a_3, a_4)$, $C = cir(a_5, a_6)$, $D = cir(a_7, a_8)$, $E = cir(a_9, a_{10})$, $F = cir(a_{11}, a_{12})$, $G = cir(a_{13}, a_{14})$, $H = cir(a_{15}, a_{16})$ and $a_i \in R$.

▪ Let $G = \langle x, y \mid x^8 = y^2 = 1,\ x^y = x^5 \rangle \cong M_{16}$. If $\alpha = \sum_{i=0}^{7} \sum_{j=0}^{1} a_{1+i+8j} y^j x^i \in RM_{16}$, then

$$\sigma(\alpha) = CIR(A, B)$$

where $A = cir(a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8)$, $B = 3 - cir(a_9, a_{10}, a_{11}, a_{12}, a_{13}, a_{14}, a_{15}, a_{16})$ and $a_i \in R$.

▪ Let $G = \langle x, y \,|\, x^8 = y^2 = 1, x^y = x^{-1} \rangle \cong D_{16}$. If $\alpha = \sum_{i=0}^{7} \sum_{j=0}^{1} a_{1+i+8j} x^i y^j \in RD_{16}$, then

$$\sigma(\alpha) = \begin{pmatrix} A & B \\ B^T & A^T \end{pmatrix}$$

where $A = cir(a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8)$, $B = cir(a_9, a_{10}, a_{11}, a_{12}, a_{13}, a_{14}, a_{15}, a_{16})$ and $a_i \in R$.

▪ Let $G = \langle x, y \,|\, x^8 = y^2 = 1, x^y = x^{-1} \rangle \cong D_{16}$. If $\alpha = \sum_{i=0}^{7} \sum_{j=0}^{1} a_{1+i+8j} y^j x^i \in RD_{16}$, then

$$\sigma(\alpha) = CIR(A, B)$$

where $A = cir(a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8)$, $B = rcir(a_9, a_{10}, a_{11}, a_{12}, a_{13}, a_{14}, a_{15}, a_{16})$ and $a_i \in R$. This second construction coming from $D_{16}$ will be denoted by $D'_{16}$.

▪ Let $G = \langle x, y \,|\, x^8 = y^2 = 1,\ x^y = x^3 \rangle \cong SD_{16}$, the semidihedral group of order 16. If $\alpha = \sum_{i=0}^{7} \sum_{j=0}^{1} a_{1+i+8j} y^j x^i \in RSD_{16}$, then

$$\sigma(\alpha) = CIR(A, B)$$

where $A = cir(a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8)$, $B = 5 - cir(a_9, a_{10}, a_{11}, a_{12}, a_{13}, a_{14}, a_{15}, a_{16})$ and $a_i \in R$.

▪ Let $G = \langle x, y \mid x^8 = 1,\ y^2 = x^8,\ x^y = x^{-1} \rangle \cong Q_{16}$. If $\alpha = \sum_{i=0}^{7} \sum_{j=0}^{1} a_{1+i+8j} y^j x^i \in RQ_{16}$, then

$$\sigma(\alpha) = \begin{pmatrix} A & B \\ C & A \end{pmatrix}$$

where $A = cir(a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8)$, $B = rcir(a_9, a_{10}, a_{11}, a_{12}, a_{13}, a_{14}, a_{15}, a_{16})$, $C = rcir(a_{13}, a_{14}, a_{15}, a_{16}, a_9, a_{10}, a_{11}, a_{12})$ and $a_i \in R$.

▪ Let $G = \langle x, y, z \mid x^4 = y^2 = z^2 = 1,\ xy = yx,\ xz = zx,\ yz = zy \rangle \cong C_4 \times C_2 \times C_2$. If $\alpha = \sum_{i=0}^{3} x^i (a_{i+1} + a_{i+5} y + a_{i+9} z + a_{i+13} yz) \in R(C_4 \times C_2 \times C_2)$, then

$$\sigma(\alpha) = P_e \otimes CIR(A, B) + P_{(1,2)} \otimes CIR(C, D)$$

where $\mathcal{G} = \{e, (1,2)\}$, $A = cir(a_1, a_2, a_3, a_4)$, $B = cir(a_5, a_6, a_7, a_8)$, $C = cir(a_9, a_{10}, a_{11}, a_{12})$, $D = cir(a_{13}, a_{14}, a_{15}, a_{16})$ and $a_i \in R$.

▪ Let $G = \langle x, y, z \mid x^4 = y^2 = z^2 = 1,\ xy = yx,\ xz = zx,\ yz = zy \rangle \cong C_4 \times C_2 \times C_2$. If $\alpha = \sum_{i=0}^{3} x^i(a_{1+4i} + a_{2+4i}y + a_{3+4i}z + a_{4+4i}yz) \in R(C_4 \times C_2 \times C_2)$, then

$$\sigma(\alpha) = CIR(A, B, C, D)$$

where $A = CIR(A_1, A_2)$, $B = CIR(B_1, B_2)$, $C = CIR(C_1, C_2)$, $D = CIR(D_1, D_2)$, $A_1 = cir(a_1, a_2)$, $A_2 = cir(a_3, a_4)$, $B_1 = cir(a_5, a_6)$, $B_2 = cir(a_7, a_8)$, $C_1 = cir(a_9, a_{10})$, $C_2 = cir(a_{11}, a_{12})$, $D_1 = cir(a_{13}, a_{14})$, $D_2 = cir(a_{15}, a_{16})$ and $a_i \in R$.

▪ Let $G = \langle x, y, z \,|\, x^4 = y^2 = z^2 = 1, x^y = x^{-1}, xz = zx, yz = zy \rangle \cong C_2 \times D_8$. If

$$\alpha = \sum_{i=0}^{3} x^i(a_{i+1} + a_{i+5}y + a_{i+9}z + a_{i+13}yz) \in R(C_2 \times D_8),$$

then

$$\sigma(\alpha) = \begin{pmatrix} A & B & C & D \\ B^T & A^T & D^T & C^T \\ C & D & A & B \\ D^T & C^T & B^T & A^T \end{pmatrix}$$

where $A = cir(a_1, a_2, a_3, a_4)$, $B = cir(a_5, a_6, a_7, a_8)$, $C = cir(a_9, a_{10}, a_{11}, a_{12})$, $D = cir(a_{13}, a_{14}, a_{15}, a_{16})$ and $a_i \in R$.

▪ Let $G = \langle x, y, z \,|\, x^4 = y^2 = z^2 = 1, x^y = x^{-1}, xz = zx, yz = zy \rangle \cong C_2 \times D_8$. If

$$\alpha = \sum_{i=0}^{3} (a_{i+1} + a_{i+5}y + a_{i+9}z + a_{i+13}yz)x^i \in R(C_2 \times D_8),$$

then

$$\sigma(\alpha) = P_e \otimes CIR(A, B) + P_{(1,2)} \otimes CIR(C, D)$$

where $\mathcal{G} = \{e, (1,2)\}$, $A = cir(a_1, a_2, a_3, a_4)$, $B = rcir(a_5, a_6, a_7, a_8)$, $C = cir(a_9, a_{10}, a_{11}, a_{12})$, $D = rcir(a_{13}, a_{14}, a_{15}, a_{16})$ and $a_i \in R$.

▪ Let $G = \langle x, y, z \mid x^4 = z^2 = 1,\ y^2 = x^2,\ x^y = x^{-1}\, xz = zx,\ yz = zy \rangle \cong C_2 \times Q_8$. If

$$\alpha = \sum_{i=0}^{3} (a_{i+1} + a_{i+5}y + a_{i+9}z + a_{i+13}yz)x^i \in R(C_2 \times Q_8),$$

then

$$\sigma(\alpha) = \begin{pmatrix} A & B & D & E \\ C & A & F & D \\ D & E & A & B \\ F & D & C & A \end{pmatrix},$$

where $A = cir(a_1, a_2, a_3, a_4)$, $B = rcir(a_5, a_6, a_7, a_8)$, $C = rcir(a_7, a_8, a_5, a_6)$,
$D = cir(a_9, a_{10}, a_{11}, a_{12})$, $E = rcir(a_{13}, a_{14}, a_{15}, a_{16})$, $F = rcir(a_{15}, a_{16}, a_{13}, a_{14})$ and $a_i \in R$.

▪ Let $G = \langle x, y, z \mid x^4 = z^2 = 1,\ y^2 = x^2,\ x^y = x^{-1}\, xz = zx,\ yz = zy \rangle \cong C_2 \times Q_8$. If

$$\alpha = \sum_{i=0}^{3} x^i (a_{i+1} + a_{i+5}y + a_{i+9}z + a_{i+13}yz) \in R(C_2 \times Q_8),$$

then

$$\sigma(\alpha) = \begin{pmatrix} A & B & D & E \\ C & A^T & F & D^T \\ D & E & A & B \\ F & D^T & C & A^T \end{pmatrix}$$

where $A = cir(a_1, a_2, a_3, a_4)$, $B = cir(a_5, a_6, a_7, a_8)$, $C = cir(a_7, a_6, a_5, a_8)$, $D = cir(a_9, a_{10}, a_{11}, a_{12})$, $E = cir(a_{13}, a_{14}, a_{15}, a_{16})$, $F = cir(a_{15}, a_{14}, a_{13}, a_{16})$ and $a_i \in R$. This second construction coming from $C_2 \times Q_8$ will be denoted by $(C_2 \times Q_8)'$.

▪ Let $G = \langle x, y, z \mid x^4 = y^2 = z^2 = 1,\ zyzx^2y = 1,\ yxyx^3 = 1,\ zxzx^3 = 1 \rangle \cong \mathcal{P}_{16}$. If $\alpha = \sum_{i=0}^{3} x^i (a_{i+1} + a_{i+5}y + a_{i+9}z + a_{i+13}yz) \in R\mathcal{P}_{16}$, then

$$\sigma(\alpha) = \begin{pmatrix} A & B & C & D \\ B & A & E & F \\ C & D & A & B \\ E & F & B & A \end{pmatrix},$$

where $A = cir(a_1, a_2, a_3, a_4)$, $B = cir(a_5, a_6, a_7, a_8)$, $C = cir(a_9, a_{10}, a_{11}, a_{12})$,
$D = cir(a_{13}, a_{14}, a_{15}, a_{16})$, $E = cir(a_{15}, a_{16}, a_{13}, a_{14})$, $F = cir(a_{11}, a_{12}, a_9, a_{10})$ and $a_i \in R$.

▪ Let $G = \langle x_i \,|\, x_i^2 = 1, x_i x_j = x_j x_i\ (i \neq i) \rangle \cong C_2^4$ where $1 \leq i, j \leq 4$. If

$$\begin{aligned} \alpha = {} & a_1 + a_2x_1 + a_3x_2 + a_4x_1x_2 + a_5x_3 + a_6x_1x_3 + a_7x_2x_3 + a_8x_1x_2x_3 + a_9x_4 + a_{10}x_1x_4 \\ & + a_{11}x_2x_4 + a_{12}x_1x_2x_4 + a_{13}x_3x_4 + a_{14}x_1x_3x_4 + a_{15}x_2x_3x_4 + a_{16}x_1x_2x_3x_4 \in RC_2^4 \end{aligned}$$

then

$$\sigma(\alpha) = P_e \otimes CIR(A, B) + P_{(1,2)(3,4)} \otimes CIR(C, D) + P_{(1,3)(2,4)} \otimes CIR(E, F) + P_{(1,4)(2,3)} \otimes CIR(G, H)$$

where $\mathcal{G} = \{e, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$, $A = cir(a_1, a_2)$, $B = cir(a_3, a_4)$, $C = cir(a_5, a_6)$, $D = cir(a_7, a_8)$, $E = cir(a_9, a_{10})$, $F = cir(a_{11}, a_{12})$, $G = cir(a_{13}, a_{14})$, $H = cir(a_{15}, a_{16})$ and $a_i \in R$.

## 5.1 Examples of Extremal Binary Self-dual Codes obtained from the constructions

In this section, we give examples obtained from group of order $1\dot{6}$. The constructions applied over the binary alphabet and to the ring $R_1$. Using $g-$circulant matrices to construct self-dual codes is a distinctive method. In the following example we use the construction $SD_{16}$.

**Example 5.** *Applying the semidihedral construction to the binary case length 32, up to equivalence, we get one extremal binary self-dual code of length 32 and one binary self-dual code of parameter* $[32, 16, 6]$. *Lifting these to the ring* $R_1$, *in other words, applying the semidihedral construction to the ring* $R_1$ *we get the following results:*

***Lifts of [32,16,6]:*** *Up to equivalence we get 14 extremal binary self-dual codes of length* 64. *Out of these, 11 are of Type II. The three Type I codes have two different weight enumerators. If we take*

$$(a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8) = (u, u, 0, 0, 0, 1, u, 1)$$

*and*

$$(a_9, a_{10}, a_{11}, a_{12}, a_{13}, a_{14}, a_{15}, a_{16}) = (u, 0, u, 0, 1, 1, 1, u),$$

*then the code obtained with the semidhedral construction over* $R_1$ *with these values has as its Gray image, a Type I extremal binary self-dual code that has a weight enumerator with* $\beta = 0$ *in* $W_{64,2}$.

*If we take*

$$(a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8) = (u, u, u, 0, 0, 1, 0, 1)$$

*and*

$$(a_9, a_{10}, a_{11}, a_{12}, a_{13}, a_{14}, a_{15}, a_{16}) = (u, 0, u, u, 1, 1, 1, 0),$$

*then we get a code with the same weight enumerator(*$\beta = 0$ *in* $W_{64,2}$.*)*

*If we take*

$$(a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8) = (u, u, u, 0, 0, 1, 0, 1)$$

*and*

$$(a_9, a_{10}, a_{11}, a_{12}, a_{13}, a_{14}, a_{15}, a_{16}) = (u, 0, u, 0, 1, 1, 1, u),$$

*then we get a Type I extremal binary self-dual code that has a weight enumerator with* $\beta = 16$ *in* $W_{64,2}$.

***Lifts of [32,16,8]:*** *Up to equivalence we get 13 extremal binary self-dual codes, of which 12 are Type II and the one Type I code has a weight enumerator with* $\beta = 16$ *in* $W_{64,2}$.

The constructions $G_{4,4}$ and $M_{16}$ use $3-$circulant and $5-$circulant matrices, respectively. When these are applied over the binary alphabet we obtain self-dual binary codes of length 32. Those are not listed in order to save space.

Table 6: The constructions $D'_{16}$ and $SD_{16}$ over $\mathbb{F}_2 + u\mathbb{F}_2$

| Construction | $r_A$ | $r_B$ | $\lvert Aut(C)\rvert$ | $\beta$ |
|---|---|---|---|---|
| $D'_{16}$ | (22221113) | (22130131) | $2^5$ | 0 |
| $D'_{16}$ | (22201111) | (02130311) | $2^5$ | 16 |
| $D'_{16}$ | (22001113) | (20132111) | $2^5$ | 32 |
| $D'_{16}$ | (22001131) | (22110133) | $2^5$ | 48 |
| $SD_{16}$ | (00332312) | (23331102) | $2^5$ | 32 |

Table 7: The construction $Q_{16}$ over $\mathbb{F}_2 + u\mathbb{F}_2$

| $r_A$ | $r_B$ | $r_C$ | $\lvert Aut(C)\rvert$ | $\beta$ |
|---|---|---|---|---|
| (20131120) | (11023321) | (00112232) | $2^4$ | 0 |
| (03003112) | (21103301) | (02311020) | $2^5$ | 0 |
| (10110221) | (33231212) | (22320303) | $2^4$ | 12 |
| (01221112) | (21323321) | (20313222) | $2^4$ | 16 |
| (10130021) | (31231032) | (00122103) | $2^4$ | 20 |
| (23021312) | (01121303) | (22333022) | $2^4$ | 32 |
| (21223310) | (21103303) | (00331220) | $2^5$ | 32 |
| (32110203) | (13013012) | (22300123) | $2^5$ | 36 |

In order to simplify the notation in tables we use 2 and 3 for $u$ and $1 + u$, respectively. When we apply the constructions $D'_{16}$ and $SD_{16}$ over $\mathbb{F}_2 + u\mathbb{F}_2$ we obtain extremal binary self-dual codes of length 64 as binary images. Those are listed in Table 6.

In Tables 7, 8 and 9 we apply the constructions $Q_{16}$, $C_2Q_8$, $P_{16}$ and $(C_2Q_8)'$, respectively.

# 6 New Extremal binary self-dual codes of length 68

We will now explain how we find new extremal binary self-dual codes of length 68 by combining the construction methods in sections 4 and 5 and an extension theorem. We first recall that, he possible weight enumerators of an extremal self-dual binary code of length 68 are determined in [6] as follows:

$$\begin{aligned} W_{68,1} &= 1 + (442 + 4\beta)\, y^{12} + (10864 - 8\beta)\, y^{14} + \cdots, 104 \le \beta \le 1358, \\ W_{68,2} &= 1 + (442 + 4\beta)\, y^{12} + (14960 - 8\beta - 256\gamma)\, y^{14} + \ldots \end{aligned}$$

Table 8: Codes by $C_2Q_8$ and $P_{16}$ over $\mathbb{F}_2 + u\mathbb{F}_2$

| Construction | $r_A$ | $r_B$ | $r_C$ | $r_D$ | $r_E$ | $r_F$ | $\lvert Aut(C)\rvert$ | $\beta$ |
|---|---|---|---|---|---|---|---|---|
| $C_2Q_8$ | (1213) | (2331) | (3123) | (0021) | (1230) | (0220) | $2^4$ | 8 |
| $C_2Q_8$ | (1233) | (0311) | (1301) | (0003) | (3032) | (0200) | $2^4$ | 24 |
| $C_2Q_8$ | (2221) | (3210) | (2301) | (3312) | (0221) | (1330) | $2^5$ | 24 |
| $C_2Q_8$ | (2001) | (1032) | (2103) | (1310) | (2003) | (1132) | $2^4$ | 40 |
| $P_{16}$ | (2010) | (0320) | (3103) | (1230) | (3311) | (3301) | $2^4$ | 8 |
| $P_{16}$ | (2310) | (0220) | (3320) | (1123) | (1231) | (2011) | $2^5$ | 8 |
| $P_{16}$ | (3021) | (1331) | (0211) | (0223) | (3022) | (3302) | $2^6$ | 8 |
| $P_{16}$ | (0212) | (0322) | (3123) | (3212) | (1333) | (3321) | $2^4$ | 24 |
| $P_{16}$ | (3223) | (3113) | (0031) | (2003) | (1220) | (1300) | $2^5$ | 24 |

Table 9: Type I extremal self-dual binary codes of length 64 via $(C_2Q_8)'$

| $r_A$ | $r_B$ | $r_C$ | $r_D$ | $r_E$ | $r_F$ | $r_G$ | $r_H$ | $\lvert Aut(C)\rvert$ | $\beta$ |
|---|---|---|---|---|---|---|---|---|---|
| (1331) | (0033) | (0330) | (0220) | (0023) | (0233) | (0332) | (3013) | $2^4$ | 8 |
| (1331) | (2013) | (2130) | (0220) | (2003) | (0013) | (0130) | (3011) | $2^4$ | 24 |

where $0 \leq \gamma \leq 9$ by [17]. The existence of codes is known for many parameters for both of the cases. In $W_{68,2}$ codes exist for $\gamma = 0, 1, 2, 3, 4$ and 6. For a list of known codes in $W_{68,2}$ we refer to [23]. In order to save space, we list only the parameters for $\gamma = 4$ in $W_{68,2}$, which is;

$$\beta \in \left\{ 2m \;\middle|\; \begin{array}{c} 43, 48, 49, 51, 52, 54, 55, 56, 58, 60, 61, 62, \\ 64, 65, 67, \ldots, 71, 75, \ldots, 88, 90, 97, 98 \end{array} \right\}.$$

In this section, we obtain 10 new extremal binary self-dual codes of length 68. More precisely, we construct codes whose weight enumerators have $\gamma = 4$ and $\beta$ =126, 129, 132, 141, 144, 145, 146, 148, 157 and 161 in $W_{68,2}$.

In order to construct new codes of length 68 we use the following extension theorem over $\mathbb{F}_2 + u\mathbb{F}_2$.

**Theorem 6.1.** *([12]) Let $\mathcal{C}$ be a self-dual code over $\mathbb{F}_2 + u\mathbb{F}_2$ of length $n$ and $G = (r_i)$ be a $k \times n$ generator matrix for $\mathcal{C}$, where $r_i$ is the $i$-th row of $G$, $1 \leq i \leq k$. Let $c$ be a unit in $\mathbb{F}_2 + u\mathbb{F}_2$ and $X$ be a vector in $(\mathbb{F}_2 + u\mathbb{F}_2)^n$ with $\langle X, X \rangle = 1$. Let $y_i = \langle r_i, X \rangle$ for $1 \leq i \leq k$. Then the following matrix*

$$\left( \begin{array}{cc|c} 1 & 0 & X \\ \hline y_1 & cy_1 & r_1 \\ \vdots & \vdots & \vdots \\ y_k & cy_k & r_k \end{array} \right),$$

*generates a self-dual code $\mathcal{C}'$ over $\mathbb{F}_2 + u\mathbb{F}_2$ of length $n + 2$.*

By the use of groups of order 8 we obtain codes of length 16 over $\mathbb{F}_4 + u\mathbb{F}_4$ with binary images as $[64, 32, 12]_2$ self-dual codes. We map the codes to the ring $\mathbb{F}_2 + u\mathbb{F}_2$ via the Gray map $\psi_{\mathbb{F}_4 + u\mathbb{F}_4}$ and extend the $\mathbb{F}_2 + u\mathbb{F}_2$-image. We ran the files for various constructions and codes. However, we were able to obtain new codes for only the following two codes:

| $\mathcal{C}_i$ | Construction | $r_A$ | $r_B$ | $\beta$ in $W_{64,2}$ | $\lvert Aut\,(\mathcal{C}_i)\rvert$ |
|---|---|---|---|---|---|
| $\mathcal{C}_1$ | $D_8$ | $(6ED7)$ | $(D40A)$ | 24 | $2^5$ |
| $\mathcal{C}_2$ | $D_8{}'$ | $(2DBE)$ | $(1174)$ | 28 | $2^4$ |

The new codes are tabulated in Table 10. In order to save space the element $1 + u$ of $\mathbb{F}_2 + u\mathbb{F}_2$ is denoted by 3 in the extension vector $X$. Thus we have the following main theorem about the existence of extremal binary self-dual codes of length 68.

**Theorem 6.2.** *Together with the codes in Table 10 the existence of extremal self-dual binary codes is known for* 46 *parameters with $\gamma = 4$ in $W_{68,2}$.*

**Remark 2.** *The codes constructed in this section are the first extremal binary self-dual codes of length* 68 *with weight enumerators for $\gamma = 4$ where $\beta$ is odd. This shows that, the construction methods we have introduced have the potential to fill the gaps that remain with other constructions applied thus far. The binary generator matrices of the new codes are available online at [16].*

Table 10: Ten new extremal self-dual codes of length 68 with $\gamma = 4$

| $\mathcal{C}_{68,i}$ | $\mathcal{C}_j$ | $c$ | $X$ | $\beta$ |
|---|---|---|---|---|
| $\mathcal{C}_{68,1}$ | $\mathcal{C}_1$ | $1+u$ | $(u31uu0uuu0uu0u303u3033333011uu3u)$ | 126 |
| $\mathcal{C}_{68,2}$ | $\mathcal{C}_2$ | 1 | $(300u11331003u1130333110u0301110u)$ | 129 |
| $\mathcal{C}_{68,3}$ | $\mathcal{C}_1$ | $1+u$ | $(u33u000000uu0u30303013311u11uu3u)$ | 132 |
| $\mathcal{C}_{68,4}$ | $\mathcal{C}_1$ | $1+u$ | $(033uuuuu000uuu3u103u13331013u030)$ | 144 |
| $\mathcal{C}_{68,5}$ | $\mathcal{C}_2$ | 1 | $(1uu011313u01u331033333u0u3u131u0)$ | 145 |
| $\mathcal{C}_{68,6}$ | $\mathcal{C}_1$ | 1 | $(011u0uuu0u0uu03u303031111033uu1u)$ | 146 |
| $\mathcal{C}_{68,7}$ | $\mathcal{C}_1$ | 1 | $(0130uuu0000u00303u1011311u13u010)$ | 148 |
| $\mathcal{C}_{68,8}$ | $\mathcal{C}_2$ | $1+u$ | $(3uu011331003u113u31131u0u30313uu)$ | 155 |
| $\mathcal{C}_{68,9}$ | $\mathcal{C}_2$ | $1+u$ | $(1u00131330u3u131u313310u0303310u)$ | 157 |
| $\mathcal{C}_{68,10}$ | $\mathcal{C}_2$ | $1+u$ | $(1uuu33133u03u133u13313u0u3u1130u)$ | 161 |

# 7 Conclusion

In this work, we established a strong connection between group rings and self-dual codes. In particular, this brought about a new motivation for studying unitary units in groups rings and their orders. We also found many new construction methods for self-dual codes coming from groups. We found that certain general groups such as cyclic groups and dihedral groups lead to the well-known and oft-used double-circulant and four-circulant constructions. We established the relevance of the new construction methods by finding many extremal binary self-dual codes using them.

We used groups of order 8 and order 16 for the construction methods. Using groups of different orders might lead to more construction methods. Different rings and their corresponding Gray maps can also be used with these constructions. Currently we cannot establish the minimum distance of the code from the corresponding group ring element. An attempt at resolving this question might be quite a relevant direction of future research in this area.

# References


[1] D. Anev, M. Haraada and N. Yankov, "New extremal singly even self-dual codes of lengths 64 and 66", arXiv:1708.05950, 2017.

[2] F. Bernhardt, P. Landrock, and O. Manz, "The extended Golay codes considered as ideals", *J. Combin. Theory Ser. A*, Vol. 55, no. 2, pp. 235–246, 1990.

[3] K. Betsumiya, S. Georgiou, T.A. Gulliver, M. Harada and C. Koukouvinos, "On self-dual codes over some prime fields", *Discrete Math*, Vol. 262, pp. 37–58, 2003.

[4] W. Bosma, J. Cannon and C. Playoust, "The Magma algebra system. I. The user language", *J. Symbolic Comput.*, Vol. 24, pp. 235–265, 1997.

[5] V. Bovdi and A.L. Rosa, "On the order of the unitary subgroup of a modular group algebra", *Comm. Algebra*, Vol. 28, no. 4, pp. 1897–1905, 2000.

[6] S. Buyuklieva, I. Boukliev, "Extremal self-dual codes with an automorphism of order 2", *IEEE Trans. Inform. Theory*, Vol. 44, pp. 323–328, 1998.

[7] J.H. Conway and N.J.A. Sloane, "A new upper bound on the minimal distance of self-dual codes", *IEEE Trans. Inform. Theory*, Vol. 36, no. 6, pp. 1319–1333, 1990.

[8] P.J. Davis, *Circulant Matrices*, Chelsea Publishing, New York (1979).

[9] S.T. Dougherty, P. Gaborit, M. Harada and P. Solé, "Type II codes over $\mathbb{F}_2 + u\mathbb{F}_2$", *IEEE Trans. Inform. Theory*, Vol. 45, pp. 32–45, 1999.

[10] S.T. Dougherty, B. Yildiz and S. Karadeniz, "Codes over $R_k$, Gray maps and their Binary Images", *Finite Fields and their Applications*, Vol. 17, no. 3, pp. 205–219, 2011.

[11] S.T. Dougherty, P. Gaborit, M. Harada and P. Sole, "Type II codes over $\mathbb{F}_2 + u\mathbb{F}_2$", *IEEE Trans. Inform. Theory*, Vol. 45, pp. 32–45, 1999.

[12] S.T. Dougherty, J.-L. Kim, H. Kulosman, H. Liu,"Self-dual codes over commutative Frobenius rings", *Finite Fields and their Applications*, Vol. 16, pp. 14–26, 2010.

[13] P. Gaborit, V. Pless, P. Sole and O. Atkin, "Type II codes over $\mathbb{F}_4$", *Finite Fields and their Applications*, Vol.8, no. 2, pp. 171–183, 2002.

[14] The GAP Group, GAP – Groups, Algorithms and Programming, Version 4.4, 2006 (http:/www.gap-system.org).

[15] J. Gildea, "The structure of the unitary units of the group algebra $\mathbb{F}_{2^k}D_8$", *IEJA*, Vol 9, pp. 171–176, 2011.

[16] J. Gildea, A. Kaya, R. Taylor and B. Yildiz "Binary generator matrices for some extremal binary self-dual codes of length 64", available online at `http://abidinkaya.wixsite.com/main/research3`

[17] M. Harada, A. Munemasa, "Some restrictions on weight enumerators of singly even self-dual codes", *IEEE Trans. Inform. Theory*, Vol. 52, pp. 1266–1269, 2006.

[18] T. Hurley, "Group Rings and Rings of Matrices", *Int. Jour. Pure and Appl. Math*, Vol. 31, no. 3, pp. 319–335, 2006.

[19] T. Hurley, "Self-dual, dual-containing and related quantum codes from group rings", arXiv:0711.3983, 2007.

[20] S. Karadeniz and B. Yildiz, "New extremal binary self-dual codes of length 64 from $R_3$ lifts of the extended binary Hamming code", *Des. Codes Cryptogr.,* Vol. 74, no. 3, pp. 673–680, 2015.

[21] S. Karadeniz, B. Yildiz and N. Aydin, "Extremal binary self-dual codes of lengths 64 and 66 from four-circulant constructions over codes $\mathbb{F}_2 + u\mathbb{F}_2$", *FILOMAT*, Vol. 28, no. 5, pp. 937–945, 2014.

[22] A. Kaya, "New extremal binary self-dual codes of lengths 64 and 66 from $R_2$-lifts", *Finite Fields and their Applications*, Vol. 46, pp. 271–279, 2017.

[23] A. Kaya, "New extremal binary self-dual codes of length 68 via the short Kharaghani array over $\mathbb{F}_2 + u\mathbb{F}_2$", *Mathematical Communications*, Vol. 22, pp. 121–131, 2017.

[24] A. Kaya, B. Yildiz and I. Siap, "New extremal binary self-dual codes from $\mathbb{F}_4 + u\mathbb{F}_4$-lifts of quadratic double circulant codes over $\mathbb{F}_4$", *Finite Fields Appl.*, Vol.35, pp.318–329, 2015.

[25] A. Kaya and B. Yildiz, "Various constructions for self-dual codes over rings and new binary self-dual codes", *Discrete Mathematics*, Vol. 339, no. 2, pp. 460–469, 2016.

[26] S. Ling and P. Sole, "Type II codes over $\mathbb{F}_4 + u\mathbb{F}_4$", *Europ. J. Combinatorics*, Vol. 22 pp. 983–997, 2001.

[27] I. McLoughlin, "A group ring construction of the $[48, 24, 12]$ Type II linear block code", *Des. Codes Cryptogr.*, Vol. 63, no. 1, pp. 29–41, 2012.

[28] I. McLoughlin and T. Hurley, "A group ring construction of the extended binary Golay code", *IEEE Trans. Inform. Theory*, Vol. 54, no. 9, pp. 4381–4383, 2008.

[29] E.M. Rains, "Shadow Bounds for Self Dual Codes", *IEEE Trans. Inform. Theory*, Vol. 44, pp.134–139, 1998.

[30] N. Yankov, "Self-dual $[62, 31, 12]$ and $[64, 32, 12]$ codes with an automorphism of order 7", *Advances in Mathematics of Communications*, Vol. 8, no. 1. pp. 73–81, 2014.